Congress of the United States
House of Representatives
SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY

March 3rd , 2025

Hui Zhao
China Telecom (Americas) Corporation
607 Herndon Pkwy STE 201
Herndon, VA 20170

Dear Mr. Zhao,

We write to address serious and ongoing national security concerns regarding China Telecom's potential activities in the United States that pose a risk to the security and privacy of Americans' communications and networks.

In 2021, the Federal Communications Commission (FCC) revoked China Telecom's U.S. Section 214 license because the company threatened the privacy and security of Americans' communications and U.S. national security because of the company's deep ties to the Chinese government and intelligence services, made all the worse by China Telecom's "lack of candor, trustworthiness, and reliability" before the FCC. Public reporting also revealed unauthorized data access, traffic misrouting, and network management failures from China Telecom's systems.[1] Just two months ago, the Biden Administration issued a notice finding that China Telecom's residual operations in the United States continue to pose a national security threat.[2]

The Committee has received information indicating that China Telecom may continue to maintain network Points of Presence (PoPs), data center access, and cloud-related offerings in the United States, potentially through China Telecom subsidiaries or affiliates. Under the PRC's National Intelligence Law, Chinese state-owned enterprises and other purportedly private

[1] FCC, *FCC Revokes and Terminates China Telecom America's Authority to Provide Telecom Services in America*, FCC.gov (Oct. 26, 2021), https://www.fcc.gov/document/fcc-revokes-china-telecom-americas-telecom-services-authority ; Phillipa Gill, *Characterizing Large-Scale Routing Anomalies: A Case Study of the China Telecom Incident*, Citizen Lab (Dec. 17, 2012), https://citizenlab.ca/2012/12/characterizing-large-scale-routing-anomalies-a-case-study-of-the-china-telecom-incident/.

[2] Biden Administration Takes First Step to Retaliate Against China Over Hack - The New York Times; Alexandra Alper, *Exclusive: US Probing China Telecom, China Mobile over Internet, Cloud Risks*, Reuters (June 25, 2024), https://www.reuters.com/business/media-telecom/us-probing-china-telecom-china-mobile-over-internet-cloud-risks-2024-06-25/.

businesses can be compelled to assist with intelligence activities.[3] China Telecom's ongoing U.S. operations—particularly in internet backbone exchanges and cloud computing environments—could therefore allow unauthorized data access, espionage, or sabotage by the Chinese Communist Party (CCP).

China Telecom's documented connections to PRC intelligence raise urgent national security questions in light of the Chinese government's increasingly aggressive attacks on U.S. telecommunications networks. PRC-linked Salt Typhoon, described by a former Chairman of the Senate Select Committee on Intelligence as "the worst telecom hack in our nation's history" compromised sensitive data of millions of Americans.[4] Volt Typhoon, tied to China's Ministry of State Security, is waging what the FBI calls China's "most significant cyber-espionage campaign in history," infiltrating U.S. critical infrastructure and telecommunications equipment and inserting malware that could cause physical harm to Americans.[5]

China Telecom also appears to play a significant role in facilitating cyber-enabled espionage and data exfiltration for CCP-linked global cyber operations. Reporting indicates that China Telecom, along with China Unicom and China Mobile, have signed formal agreements with cybercriminal actors that enable access to sensitive data.[6] These arrangements suggest an active role by China Telecom and its affiliates in fostering illicit relationships with cyber threat actors. Such collaborations allow criminal entities to trade stolen data more efficiently, shield their activities from detection, and continue cyber-enabled operations against international targets, including U.S. businesses and government entities.

Reports indicate that China Telecom's network infrastructure has been leveraged by PRC-affiliated cybercriminals to facilitate large-scale data theft, often involving critical personal, corporate, and government data.[7] The illegal data trade network, estimated to be worth over 150 billion yuan, continues to thrive due to the ease with which threat actors exploit international communication channels.[8] In some cases, compromised software development kits (SDKs), which are integrated into widely used applications, serve as persistent access points for continued data extraction.[9] The infrastructure provided by China Telecom has been observed in facilitating

---

[3] Rogier Creemers, Graham Webster & Paul Triolo, Translation: "*Cybersecurity Law of the People's Republic of China (Effective June 1, 2017),"* DigiChina (June 29, 2018), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
[4] Mike Brest, *Senate Intel chairman call Chinese hack 'worst' in 'nation's history'"*, Washington Examiner (Nov. 22, 2024), https://www.washingtonexaminer.com/policy/defense/3238943/senate-intel-chairman-chinese-hack-worst-nation-history/.
[5] Andy Greenberg, "*China's Salt Typhoon Spies Are Still Hacking Telecoms—Now by Exploiting Cisco Routers*," Wired (Feb. 13, 2025), https://www.wired.com/story/chinas-salt-typhoon-spies-are-still-hacking-telecoms-now-by-exploiting-cisco-routers/.
[6] Kyla Cardona & Ashley Allocca, *"Pantsless Data": Decoding Chinese Cybercrime TTPs*, SpyCloud (Feb. 26, 2024), https://spycloud.com/blog/growing-chinese-threat-actor-ecosystem/.
[7] *Id.*
[8] *Id.*
[9] *Id.*; *see also* Kyle Cardona, "*A Deep Dive Into the Intricate Chinese Cybercrime Ecosystem*," SpyCloud (Oct. 18, 2024), https://spycloud.com/blog/deep-dive-chinese-cybercrime-ecosystem/.

these operations, enabling PRC cyber actors to disguise their activities and obfuscate attribution.[10]

We therefore write today to request detailed information about China Telecom's continued operations in the United States to assess the risks such activities pose to American national security. Specifically, we request that you provide the following information by March 31st, 2025:

1) Documents and records that provide a complete and comprehensive record of all of China Telecom's physical or virtual infrastructure and related offerings in the United States.
    a) Please produce documents and records that provide a comprehensive and detailed explanation of the PoPs, data center facilities, partnerships, and other physical or virtual infrastructure that China Telecom and its subsidiaries and affiliates operate within the United States.
2) All documents, records, agreements, contracts, or similar materials between China Telecom or one of its subsidiaries or affiliates to provide internet, cloud connectivity, or enterprise services to customers in the United States.
    a) These documents and records should include all contracts, agreements, or similar materials related to direct connect services with major U.S. cloud providers.
3) All documents, records, and communications related to any internal or external investigations, audits, or incident reports conducted in the past three years regarding inadvertent or intentional rerouting of U.S. internet traffic through Chinese networks or unauthorized data access at China Telecom or one of its subsidiaries or affiliates.
4) All documents, records, and communications related to your company's compliance with the FCC revocation order and any other relevant instructions from U.S. agencies, including timelines and correspondence.
5) All documents, records, and communications related to all protocols your company has in place to prevent unauthorized access, interception, or manipulation of data traversing your U.S. networks, including any cloud computing services operated by China Telecom. Explain any steps taken to ensure U.S. customer data is stored and protected in compliance with American laws.
6) **PRC government contracts:**
    a) Does your company, its parent or any affiliate or subsidiary of your company or its parent have any current contracts with the PRC government? If so, please produce a copy of all such agreements.

[10] *Id.*

b) Has your company, its parent or any affiliate or subsidiary of your company or its parent had any contracts with the PRC government over the last five years? If so, please produce a copy of all such agreements.

c) Has your company entered into any research agreements with any entity that is subject to the direction or control of the PRC government or one of its organs? If so, please produce documents and information sufficient to provide detailed information about such research agreements.

d) Has the PRC government—through a contractual mechanism, regulatory requirement, or formal or informal request, or any other means—ever requested that you or your parent or a subsidiary or affiliate of your company or your parent company modify the products or services provided by your company, its parent, or a subsidiary or affiliate of your company or its parent? Please produce documents and information sufficient to explain the modification requested and the reason for such modification.

e) Has your company or its parent or an affiliate or subsidiary of your company or its parent received any PRC government or CCP awards, honors, or subsidies of any kind? Please produce documentation of the award, honor, or subsidy and records verifying the total amount received and conditions of receipt, if any.

7) **Collaboration with PRC military, intelligence authorities or blacklisted entities:**

a) Please describe with specificity any engagement, partnership, research or contractual relationship, or other relationship between your company (parent/subsidiary/affiliate) and any of the following. For each relationship, produce documents or information sufficient to identify the key officials with whom your company (parent/subsidiary/affiliate) engaged. Please also produce all documents describing such engagement, research, or contractual or other formal relationship.

i) The People's Liberation Army and any of its components or subordinate entities;

ii) The Ministry of National Defense and any component or subordinate entities;

iii) The Central Military Commission and any component or subordinate entities;

iv) The Ministry of State Security and any component or subordinate entities; or

v) The Ministry of Public Security and any component or subordinate entities.

b) Please list all meetings that your company (or parent/subsidiary/affiliate) has had with officials from any of the above-listed entities in the past five years, including the names and titles of all relevant participants.

c) Does your company (or parent/subsidiary/affiliate) have any contractual relationships—including customer agreements, supplier or sub-tier supplier agreements, or research collaborations—with any PRC entities listed on a U.S. government blacklist, including

the Section 1260H of the 2021 National Defense Authorization Act (NDAA), Bureau of Industry and Security (BIS) Entity List, Uyghur Forced Labor Prevention Act (UFLPA) Entity List, Commerce Department's Military End User List, Executive Order 14059, Specially Designated Nationals and Blocked Persons (SDN) List, Non-SDN Chinese Military-Industrial Complex (NS-CMIC) Companies List, etc.? If so, please produce all such agreements.

d) Has your company (parent/subsidiary/affiliate) collaborated with any PRC universities involved in defense or intelligence related research? If so, please describe the nature of that collaboration and produce all relevant documentation establishing or governing that relationship.

e) Has your company (parent/subsidiary/affiliate) purchased any products from U.S. companies that require an export license? If so, please produce all relevant documentation related to such purchases, including licensing information and information related to the end use of such products.

f) Has your company participated in any programs, partnerships, collaborations, or other initiatives associated with China's Military-Civil Fusion strategy? If so, please produce all documents related to such participation and the names of the individuals and organizations with whom that participation occurred.

g) Has your company participated in any programs, partnerships, collaborations, or other initiatives associated with China's Belt and Road Initiative? If so, please produce all documents related to such participation and the names of the individuals and organizations with whom that participation occurred.

8) **Chinese Communist Party links:**

a) Please produce a list of all employees of China Telecom (Americas), the company's parents, and affiliates who are members of the CCP.

b) Please produce a list of all individuals on your company (or its parent/subsidiary /affiliates) internal CCP committee. Please identify the leadership of the committee including names and titles.

c) Do any of your employees who are CCP members hold a position in any CCP party organizing body at the national, state, or local level? Please identify the relevant individuals, their positions at your company (parents/subsidiary/affiliate), and their role in the relevant Party entity.

d) Please describe with specificity all engagements your company (or parent/subsidiary/affiliate etc.) has had with the CCP and its representative bodies. Please produce a list of all meetings with CCP national or regional officials within the last five years. Please include the nature of the engagement, topic(s) discussed or addressed, the

names of the corporate representatives and CCP officials who attended the relevant engagement, and their respective titles.

The House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party has broad authority to investigate and submit policy recommendations on countering the economic, technological, security, and ideological threats of the Chinese Communist Party to the United States and allies and partners of the United States under H. Res. 5 Sec. 4(a).

We appreciate your prompt attention to this matter and your full cooperation by March 31st 2025. Should you have any questions or wish to discuss this request, please contact the Committee majority and minority staff at (202) 226-9678 and (202) 225-2489, respectively.

Sincerely,

John Moolenaar
Chairman

Raja Krishnamoorthi
Ranking Member